This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Previously presented) A method comprising:

receiving data from a network application program interface (API);

determining if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data;

creating a selector based on the selector data, wherein said selector indicates at least a portion of the data and a security association;

applying the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data; and

sending the data to which the security operation has been applied to a network protocol layer.

2. (Previously presented) The method of claim 1 further comprising:

using said selector to search a database of security associations for at least one selector/security association pair identifying a security association corresponding to the selector.

3. (Previously presented) The method of claim 1 wherein the selector data is based at least in part on one of an internet protocol address taken from the data and a port indicator taken from the data.

4. (Previously presented) The method of claim 1 wherein applying the security operation comprises at least one of:

attaching a header to the data, said header including a security operation tag;

performing an integrity check; and

encrypting the data.

5. (Previously presented) The method of claim 1 wherein determining if the data is eligible for the security operation and applying the security operation if the data is eligible depends, at least in part upon a local selector/security association pair at a sending client corresponding to a remote selector/security association pair at a receiving client, said local selector/security association pair and said remote selector/security association pair having been received from a key server.

6. (Previously presented) A method comprising:

receiving data from a network protocol layer;

determining if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data;

creating a selector based on the selector data, said selector indicating at least a portion of the data and a security association;

applying the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data; and

sending the data to which the security operation has been applied to a network application program interface (API).

7. (Original) The method of claim 6 wherein determining if the data is eligible for a security operation comprises at least one of:

detecting a security operation tag in a header of the data; and

detecting failure of an integrity check on the data.

8. (Previously presented) The method of claim 6 further comprising:

using said selector to search a database of security associations for at least one selector/security association pair identifying a security association corresponding to the selector.

9. (Original) The method of claim 8 further comprising:

blocking the data from being sent to the network API if no security association corresponding to the selector is found.

10. (Original) The method of claim 6 wherein determining if the data is eligible for the security operation comprises:

determining that the data is not eligible for the security operation if a selector that references a database of security associations cannot be created based on the data.

11. (Previously presented) The method of claim 6 wherein determining if the data is eligible for the security operation comprises:

blocking the data from being send to the network API if the data includes selector data but no selector can be created from it.

12. (Canceled)

13. (Previously presented) The method of claim 6 wherein the security association comprises at least one of:

applying encryption to the data;

removing special packaging from the data;

applying decryption to the data; and

performing an integrity check on the data.

14. (Previously presented) A machine readable storage medium having stored thereon machine executable instructions, execution of said machine executable instructions being operable to implement a method comprising:

receiving data from a network application program interface (API);

determining if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data;

creating a selector based on the selector data, wherein said selector indicates at least a portion of the data and a security association;

applying the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data; and

sending data to which the security operation has been applied to a network protocol layer.

15. (Previously presented) The machine readable storage medium of claim 14 further comprising:

using said selector to search a database of security associations, for at least one selector/security association pair identifying a corresponding a security association.

16. (Previously presented) The machine readable storage medium of claim 14 wherein the selector data is based at least in part on one of an internet protocol address taken from the data and a port indicator taken from the data.

17. (Previously presented) The machine readable storage medium of claim 14 wherein applying the security operation comprises at least one of:

attaching a header to the data, said header including a security operation tag;

performing an integrity check; and

encrypting the data.

18. (Previously presented) The machine readable storage medium of claim 14 wherein determining if the data is eligible for the security operation and applying the security operation if the data is eligible depends upon a local selector/security association pair at a sending client corresponding to a remote selector/security association pair at a receiving client, said local selector/security association pair and said remote selector/security association pair having been received from a key server.

19. (Currently amended) A machine readable storage medium having stored thereon machine executable instructions, execution of said machine executable instructions being operable to implement a method comprising:

receiving data from a network protocol layer;

determining if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data;

creating a selector based on the selector data, said selector indicating at least a portion of the data and [[the]] a security association;

applying the security operation to the data if the data is eligible, wherein applying the security operation comprises using a security association on the at least a portion of the data; and

sending the data to which the security operation has been applied to a network application program interface (API).

20. (Currently amended) The machine readable storage medium of claim 19 wherein determining if the data is eligible for a security operation comprises at least one of:

detecting a security operation tag in a header of the data; and

detecting failure of an integrity check on the data.

21. (Currently amended) The machine readable storage medium of claim 19 further having stored thereon machine executable instruction, execution of said machine executable instruction being operable to implement a method further comprising:

using said selector to search a database of security associations for at least one selector/security association pair identifying a security association corresponding to the selector.

22. (Currently amended) The machine readable storage medium of claim 21 further comprising:

blocking the data from being sent to the network API if no security association corresponding to the selector is found.

23. (Currently amended) The machine readable storage medium of claim 19 wherein determining if the data is eligible for the security operation comprises:

determining that the data is not eligible for the security operation if a selector that references a database of security associations cannot be created based on the data.

24. (Currently amended) The machine readable storage medium of claim 19 wherein determining if the data is eligible for the security operation comprises:

blocking the data from being send to the network API if the data includes selector data but no selector can be created from it.

25. (Canceled)

26. (Currently amended) The machine readable storage medium of claim 19 ~~method of claim 6~~ wherein the security association comprises at least one of :

applying encryption to the data;

removing special packaging from the data;

applying decryption to the data; and

performing an integrity check on the data.

27. (Currently amended) A management server apparatus comprising:

a processing unit to:

receive data from a network application program interface (API),

determine if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data,

create a selector based on the selector data, wherein said selector indicates at least a portion of the data and a security association,

apply the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data,

~~apply the security operation to the data if the data is eligible,~~ and

send the data to which the security operation has been applied to a network protocol layer.

28. (Previously presented) A management server apparatus comprising:

a processing unit to:

receive data from a network protocol layer,

determine if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data,

create a selector based on the selector data, said selector indicating at least a portion of the data and a security association;

apply the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data, and

send the data to which the security operation has been applied to a network application program interface (API).